

PEMBANGUNAN SISTEM PENYELAMATAN DOKUMEN YANG DISANDERA MALWARE

TUGAS AKHIR

Diajukan Untuk Memenuhi Sebagian Persyaratan
Mencapai Derajat Sarjana Teknik Informatika



oleh:

Ronald Budi Gunawan
04 07 04366

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI
UNIVERSITAS ATMA JAYA YOGYAKARTA
YOGYAKARTA
2010

Tugas Akhir berjudul

**PEMBANGUNAN SISTEM PENYELAMATAN DOKUMEN YANG
DISANDERA MALWARE**

dinyatakan telah memenuhi syarat
pada tanggal Februari 2010

Pembimbing I,



(Kusworo Anindito, S.T., M.T.)

Pembimbing II,



(Y. Sigit Purnomo WP., S.T., M.Kom.)

Tim penguji:

Penguji I,



(Kusworo Anindito, S.T., M.T.)

Penguji II,



(Th. Devi Indriasari, S.T., M.Sc.)

Penguji III,



(Eddy Julianto, S.T., M.T.)

Yogyakarta, Februari 2010
Universitas Atma Jaya Yogyakarta
Fakultas Teknologi Industri

Dekan,



(Ir. B. Kristyanto, M.Eng., Ph.D.)

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena berkat bantuan-Nya, penulis dapat mengerjakan tugas akhir dengan lancar dan dapat menyelesaikan laporan ini dengan baik.

Laporan yang berjudul *Pembangunan Sistem Penyelamatan Dokumen yang Disandera Malware* ini penulis susun sebagai salah satu syarat mencapai derajat Sarjana Teknik Informatika di Universitas Atma Jaya Yogyakarta.

Selama pengerjaan tugas akhir dan penulisan laporan ini, penulis menemui banyak hambatan. Hambatan-hambatan itu dapat diselesaikan dengan bantuan berbagai pihak. Oleh karena itu, sudah sepantasnya penulis mengucapkan banyak terima kasih kepada pihak-pihak berikut, yang telah membantu penulis:

1. Bapak Ir. B. Kristyanto, M.Eng., Ph.D., selaku Dekan Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta,
2. Bapak Kusworo Anindito, S.T., M.T., selaku Ketua Program Studi Teknik Informatika Universitas Atma Jaya Yogyakarta sekaligus dosen pembimbing I penulis, yang telah mengizinkan penulis untuk melaksanakan tugas akhir dan telah membimbing penulis selama pengerjaan tugas akhir dan penulisan laporan ini,
3. Bapak B. Yudi Dwiandiyanto, S.T., M.T., selaku Wakil Ketua Program Studi Teknik Informatika Universitas Atma Jaya Yogyakarta,
4. Bapak Y. Sigit Purnomo WP., S.T., M.Kom., selaku dosen pembimbing II penulis, yang telah

membimbing penulis selama pengerjaan tugas akhir dan penulisan laporan ini, dan

5. keluarga dan teman-teman yang senantiasa memberikan dukungan kepada penulis.

Penulis juga menyadari bahwa tulisan ini masih jauh dari sempurna. Oleh karena itu, kritik dan saran pembaca sangat penulis harapkan demi sempurnanya tulisan penulis selanjutnya.

Yogyakarta, Februari 2010

Penulis



DAFTAR ISI

HALAMAN PENGESAHAN	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR TABEL	viii
DAFTAR GAMBAR	ix
INTISARI	x
BAB I PENDAHULUAN	1
I.1. Latar Belakang	1
I.2. Perumusan Masalah	4
I.3. Batasan Masalah	5
I.4. Tujuan	5
I.5. Metode Penelitian	5
I.6. Sistematika Penulisan	6
BAB II LANDASAN TEORI	8
II.1. <i>Malware</i>	8
II.1.1. Definisi <i>Malware</i>	8
II.1.2. Dampak <i>Malware</i>	8
II.1.3. Alasan "Mewabahnya" <i>Malware</i>	9
II.1.4. Jenis <i>Malware</i>	12
II.1.5. Sejarah <i>Malware</i>	13
II.1.6. Perkembangan <i>Malware</i>	17
II.2. <i>DLL Injection</i> dan <i>API Hooking</i>	17
II.2.1. Contoh: <i>Subclassing</i> Jendela Proses Lain	18
II.2.2. <i>DLL Injection</i> Melalui <i>Registry</i>	22
II.2.3. <i>DLL Injection</i> Melalui <i>Windows Hook</i>	24
II.2.4. <i>DLL Injection</i> Melalui <i>Remote Thread</i>	27
II.2.5. <i>DLL Injection</i> dengan <i>DLL Trojan</i>	34
II.2.6. <i>DLL Injection</i> Sebagai <i>Debugger</i>	34
II.2.7. <i>DLL Injection</i> dengan <i>CreateProcess</i>	35
II.2.8. <i>API Hooking</i>	36
II.2.8.1. <i>API Hooking</i> dengan Penimpanan Kode	38
II.2.8.2. <i>API Hooking</i> dengan Perubahan <i>Import</i> <i>Section Modul</i>	40
II.3. <i>Virtualisasi</i>	44
II.3.1. Pengantar <i>Virtualisasi</i>	44
II.3.2. Sejarah <i>Virtualisasi</i>	45
II.3.3. Manfaat <i>Virtualisasi</i>	48
II.3.4. Pengantar <i>Virtual Machine</i>	49
II.3.5. Manfaat <i>Virtual Machine</i>	49
II.4. <i>Internet</i> dan <i>World Wide Web</i>	51
II.4.1. <i>Internet</i>	51

II.4.2. World Wide Web	52
BAB III ANALISIS DAN PERANCANGAN SISTEM	53
III.1. Lingkup Masalah	53
III.2. Perspektif Produk	53
III.2.1. Antarmuka Sistem	53
III.2.2. Antarmuka Pemakai	53
III.2.3. Antarmuka Perangkat Keras	54
III.2.4. Antarmuka Perangkat Lunak	54
III.2.5. Antarmuka Komunikasi	56
III.3. Fungsi Produk	56
III.4. Aliran Informasi	58
III.4.1.1. DFD Level 0 (Diagram Konteks) PANDORA	58
III.4.1.2. DFD Level 1 Proses PANDORA	59
III.4.1.3. DFD Level 2 Proses Antarmuka Web	60
III.4.1.4. DFD Level 2 Proses Penjadwal	61
III.4.1.5. DFD Level 2 Proses Penyelamat	61
III.4.1.6. DFD Level 3 Proses Menampilkan Rincian Pekerjaan Penyelamatan	62
III.4.1.7. DFD Level 3 Proses Mengelola Pekerjaan Penyelamatan	63
III.5. Kamus Data	64
III.6. <i>Entity-Relationship Diagram</i>	66
III.7. Dekomposisi Modul	66
BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM	67
IV.1. Implementasi Subsistem Antarmuka Web	67
IV.1.1. <i>File</i> Pembangun Subsistem	67
IV.1.2. Halaman untuk Anonim	68
IV.1.2.1. Halaman Pengajuan <i>File</i>	68
IV.1.2.2. Halaman Pengajuan <i>File</i> Berhasil	68
IV.1.2.3. Halaman Informasi dan Status Penyelamatan <i>File</i>	69
IV.1.2.4. Halaman <i>Login</i>	70
IV.1.2.5. Halaman <i>Login</i> Berhasil	71
IV.1.3. Halaman untuk Administrator	71
IV.1.3.1. Halaman Pengelolaan <i>File</i>	71
IV.1.3.2. Halaman Informasi dan Status Penyelamatan <i>File</i>	72
IV.1.3.3. Halaman Catatan Penyelamatan	73
IV.1.3.4. Halaman <i>Logout</i>	74
IV.2. Implementasi Subsistem Penjadwal	74
IV.2.1. <i>File</i> Pembangun Subsistem	75
IV.2.2. Algoritma Subsistem	75
IV.3. Implementasi Subsistem Penyelamat	76
IV.3.1. <i>File</i> Pembangun Subsistem	76
IV.3.2. Algoritma Subsistem	76
IV.4. Pengujian Sistem	77
IV.4.1. Perangkat Lunak Pengujian	77
IV.4.2. Perangkat Keras Pengujian	77

IV.4.3. Material Pengujian	78
IV.4.4. Sumber Daya Manusia	78
IV.4.5. Deskripsi dan Hasil Pengujian	79
IV.5. Analisis Kelebihan dan Kekurangan Sistem	87
IV.5.1. Kelebihan Sistem	87
IV.5.2. Kekurangan Sistem	87
BAB V KESIMPULAN DAN SARAN	89
V.1. Kesimpulan	89
V.2. Saran	89
DAFTAR PUSTAKA	91



DAFTAR TABEL

Tabel 3.1. Kamus Data	64
Tabel 4.1. <i>File</i> Pembangun Subsistem Antarmuka Web	67
Tabel 4.2. <i>File</i> Pembangun Subsistem Penjadwal	75
Tabel 4.3. <i>File</i> Pembangun Subsistem Penyelamat	76
Tabel 4.4. Deskripsi dan Hasil Pengujian	79



DAFTAR GAMBAR

Gambar 2.1. Proses B mencoba men- <i>subclass</i> jendela milik proses A	20
Gambar 3.1. DFD <i>Level</i> 0 PANDORA	58
Gambar 3.2. DFD <i>Level</i> 1 PANDORA	59
Gambar 3.3. DFD <i>Level</i> 2 Antarmuka Web	60
Gambar 3.4. DFD <i>Level</i> 2 Penjadwal	61
Gambar 3.5. DFD <i>Level</i> 2 Penyelamat	61
Gambar 3.6. DFD <i>Level</i> 3 Menampilkan Rincian Pekerjaan Penyelamatan	62
Gambar 3.7. DFD <i>Level</i> 3 Mengelola Pekerjaan Penyelamatan	63
Gambar 3.8. <i>Entity-Relationship Diagram</i>	66
Gambar 3.9. Arsitektur Modul	66
Gambar 4.1. Halaman Pengajuan <i>File</i>	68
Gambar 4.2. Halaman Pengajuan <i>File</i> Berhasil	69
Gambar 4.3. Halaman Informasi dan Status Penyelamatan <i>File</i>	70
Gambar 4.4. Halaman <i>Login</i>	70
Gambar 4.5. Halaman <i>Login</i> Berhasil	71
Gambar 4.6. Halaman Pengelolaan <i>File</i>	72
Gambar 4.7. Halaman Informasi dan Status Penyelamatan <i>File</i>	73
Gambar 4.8. Halaman Catatan Penyelamatan	74
Gambar 4.9. Halaman <i>Logout</i>	74
Gambar 4.10. Algoritma Subsistem Penjadwal	75
Gambar 4.11. Algoritma Subsistem Penyelamat	76

INTISARI

Dewasa ini, teknologi informasi berkembang dengan demikian pesatnya di seluruh dunia. Sebagaimana perkembangan teknologi pada umumnya, perkembangan teknologi informasi juga diikuti dengan "perkembangan" sisi negatifnya. Dalam kasus teknologi informasi, hal itu terjadi dalam bentuk "perkembangan" kejahatan teknologi informasi (*cybercrime*). Salah satu bentuk *cybercrime* adalah penciptaan dan peredaran *malware*. *Malware* merupakan program komputer yang diciptakan dan diedarkan untuk tujuan kejahatan. Salah satu jenis *malware* yang cukup menjengkelkan adalah *malware-malware* "penyandera" dokumen. Selama ini, para pengguna komputer mengatasi *malware-malware* semacam itu dengan aplikasi anti-*malware*. Meskipun aplikasi-aplikasi anti-*malware* terus dikembangkan oleh para produsennya, aplikasi-aplikasi anti-*malware* masih memiliki beberapa keterbatasan utama. Penelitian ini bertujuan untuk mengembangkan sistem yang dapat menyelamatkan dokumen yang "disandera" *malware* secara otomatis, yang sekaligus mudah diakses dan digunakan para pengguna komputer. Dengan sistem seperti itu, diharapkan para pengguna komputer dapat menyelamatkan dokumen-dokumen mereka yang "disandera" *malware*. Penelitian ini akan dilaksanakan dalam empat tahap, yaitu tahap studi pustaka, tahap analisis dan perancangan sistem, tahap implementasi sistem, serta tahap pengujian sistem. Yang akan mendapatkan manfaat dari penelitian ini adalah para pengguna komputer pada umumnya. Sementara itu, keluaran yang akan dihasilkan penelitian ini adalah berupa perangkat lunak (terdiri atas program dan kode sumbernya) serta laporan tugas akhir.

Kata kunci: penyelamatan dokumen, *malware*, *hooking* Windows API, *virtual machine*, sistem berbasis web.